HUMAN FACTORS AND SECURITY

Why Human Factors?

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)"

Humans Are Not Good At

- Calculation
  - Cannot perform cryptographic operations
  - Cannot execute authentication protocols
- Memorizing
  - Cannot remember cryptographic keys
  - Cannot remember secure passwords

Humans Are Not Good At (2)

- Knowing about all the possible consequences of their decisions
- Knowing all the technical details
  - Example: parsing URLs
- Using rational analysis
  - In many situations, emotional response takes over
  - Authority can override normal judgement

Why Users Fail?

- Impossible demands
  - Remembering complex passwords
  - Performing complex operations
- Not willing
  - People who follow security policy will leave impression of being paranoid and anal

Why Users Fail (2)

- Errors through inattention
  - Automatically clicking OK
- Following the wrong rule
- Cognitive reasons – do not understand the problem
  - Example: issues with HTTPS protocol, web server certificates, browser hacks

Social Engineering

- Hacking the people

- The Art of Deception: Controlling the Human Element of Security
  - Kevin Mitnick
- The Big Con: The Story of the Confidence Man
  - David Maurer

Social Engineering (2)

- People want to be helpful
  - Helping people who need to get work done
  - People want to return favours
- People trust colleagues
  - When you are inside the perimeter, people assume that you are authorized
  - When you know the lingo, you are trusted
- Small actions can add up to security breach

Social Engineering (3)

- People want easy money
  - In-person con games
  - Nigerian scam
  - „You have won at lottery”
  - Pyramid schemes
- People are curious
  - Experiment: memory sticks distributed. Half of senior executives put it inside their computers
  - Running e-mail attachments, clicking links

Social Engineering (4)

- People can be scared
  - „Your account at PayPal was compromised”
  - „There was suspicious activity on your credit card”
- People do not understand technical details
  - Bogus websites
  - Bogus e-mails
- Phishing: acquiring sensitive information by masquerading as a trustworthy entity

Notes on Security and Usability

- with help of Peter Gutmann

Things That Make Us Smart

- Arguably the most usable piece of security technology ever

- Ignition key tells the car when to start
  - Security is a free extra

Things That Make Us Stupid

- This works in reverse too…
  - Instead of acting as enablers/force multipliers, bad designs can reduce our effectiveness
- Technology isn't always appropriately designed, and can have quite the opposite effect to the one intended
  - This has proven particularly problematic in security user interfaces
  - Designed purely by geeks for geeks

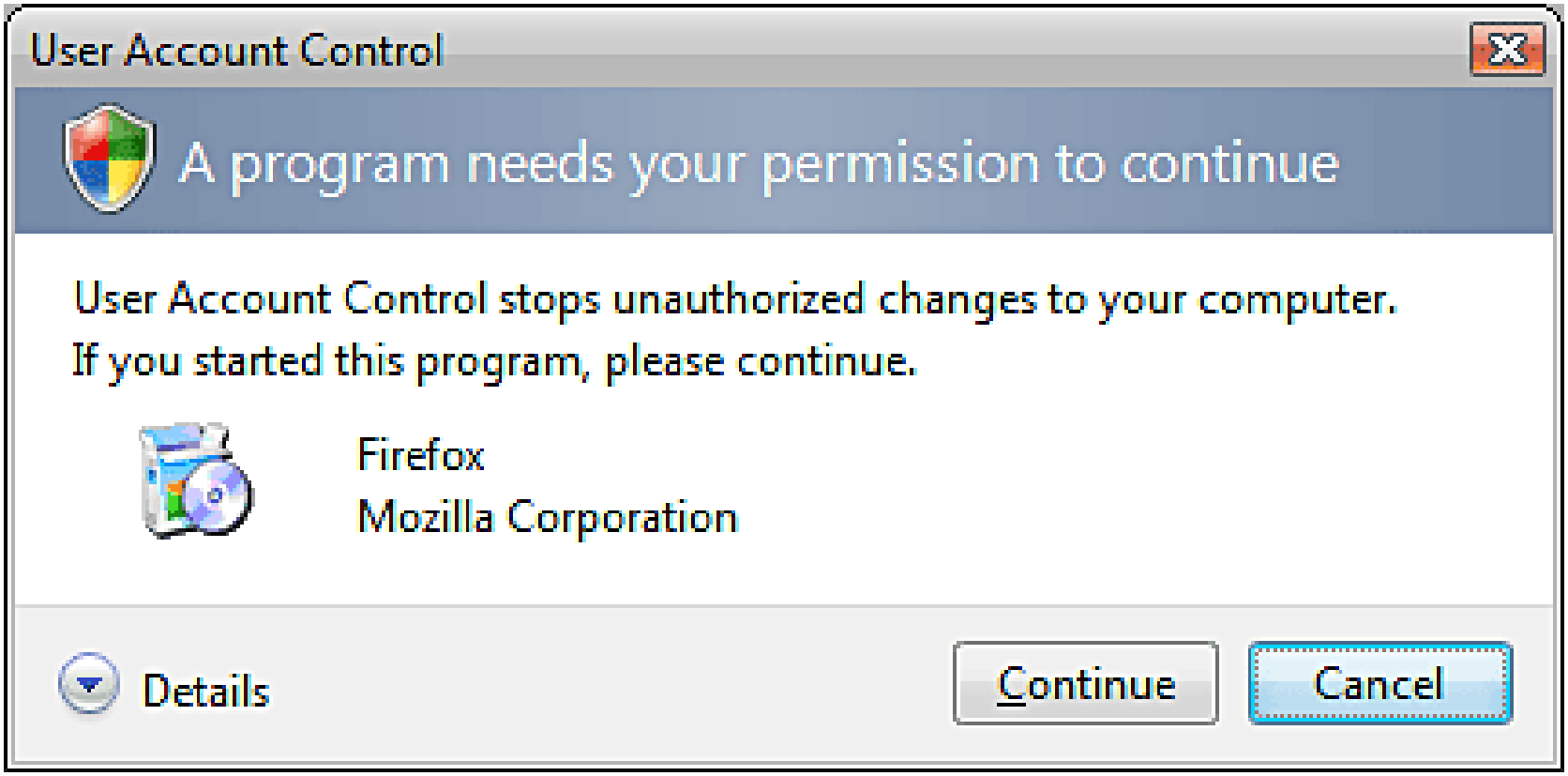
Things that Make Us Stupid

- How do you know it's a bad design?
- Effects of good design + stupid users is indistinguishable from bad design + smart users
- Definition: "Smart"
  - How geeks wish that users would behave
- Definition : "Stupid"
  - ¬ (How geeks wish that users would behave)
- Users are "stupid" simply because they don't behave in the manner arbitrarily tagged "smart" that's defined as "How users should be using my software, dammit!"

Ding-ding, and Away!

- In UK rail systems the guard signals the driver that the train can leave the station with two rings on a bell or buzzer
  - "Ding-ding!"
- Drivers became conditioned into pulling away as soon as they heard the signal
  - "Ding-ding, and away!"
- Could not be fixed because of disputes over the role of guard and driver
  - Finally fixed in 1980 after accident with 7 deaths

Click-click, and Away?



User Conditioning

- Psychologists distinguish between two types of actions taken in response to a situation
- Controlled processes
  - Slow and costly in terms of mental effort
  - Provide a great deal of flexibility in handling unexpected situations
- Automatic processes
  - Quick, little mental overhead
  - Acting on autopilot, little control or flexibility

User Conditioning (2)

- Example: Novice vs. experienced drivers
  - Novice driver has to manually and consciously check mirrors, change gears, …
  - Experienced driver performs these as an automatic process
  - Novice drivers deal with this by load-shedding
    - Sacrifice driving speed for steering control

User Conditioning (3)

- Automatic processes are people acting on autopilot
  - Once the correct stimulus is presented, it's very hard to stop
- People click away warning dialogs without thinking
  - This is an automatic process, performed without conscious awareness
- The action is not only automatic, but people aren't even aware afterwards that they've done it
  - "Did I lock the door/leave the iron on/…?"

Confirmation Bias

- Humans are bad at generating testable hypotheses
  - Phenomenon is called confirmation bias
  - Try and prove, rather than disprove, a theory
- Humans will look for (or cook) the facts in order to support the conclusions that they want to reach
  - Dissonance-motivated selectivity, look for material that avoids cognitive dissonance (challenging your opinions)

Confirmation Bias (2)

- How do you check whether a web site is valid?
  - Enter your name and password
  - If the site accepts the password, it's valid
- If the security geeks had actually designed the mechanisms properly, this would be a valid site test
  - TLS-PSK mechanism provides mutual authentication of client (browser) and (web) server without revealing the password or other shared secret
- (Little-used because it renders PKI superfluous)

Other Biases

- Disconfirmation bias
  - People are more likely to accept an invalid but plausible conclusion than a valid but implausible one
    - "This site looks and acts like my bank site, even if it's in eastern Europe. The browser must have got the URL wrong or something"
- Blind-spot bias
  - We can't see our own cognitive biases
- You just can't win!

Other Biases (2)

- The other side has authenticated themselves, from now on we can trust anything that they send us
- Has hit numerous SSH implementations (client and server)
  - Only check data validity before the user-auth phase
  - The peer would never dream of authenticating itself and only then sending a malformed packet

Other Biases (3)

- Widespread in other implementations as well
  - Unix access control: Only check security on the first access
  - Signed ActiveX controls: It's signed, it's gotta be OK
    - Signed anything: All it means is that someone paid a CA for a magic token to turn off the warning dialogs
  - Firewalls and the firewall mentality
  - …

Geeks vs. Humans

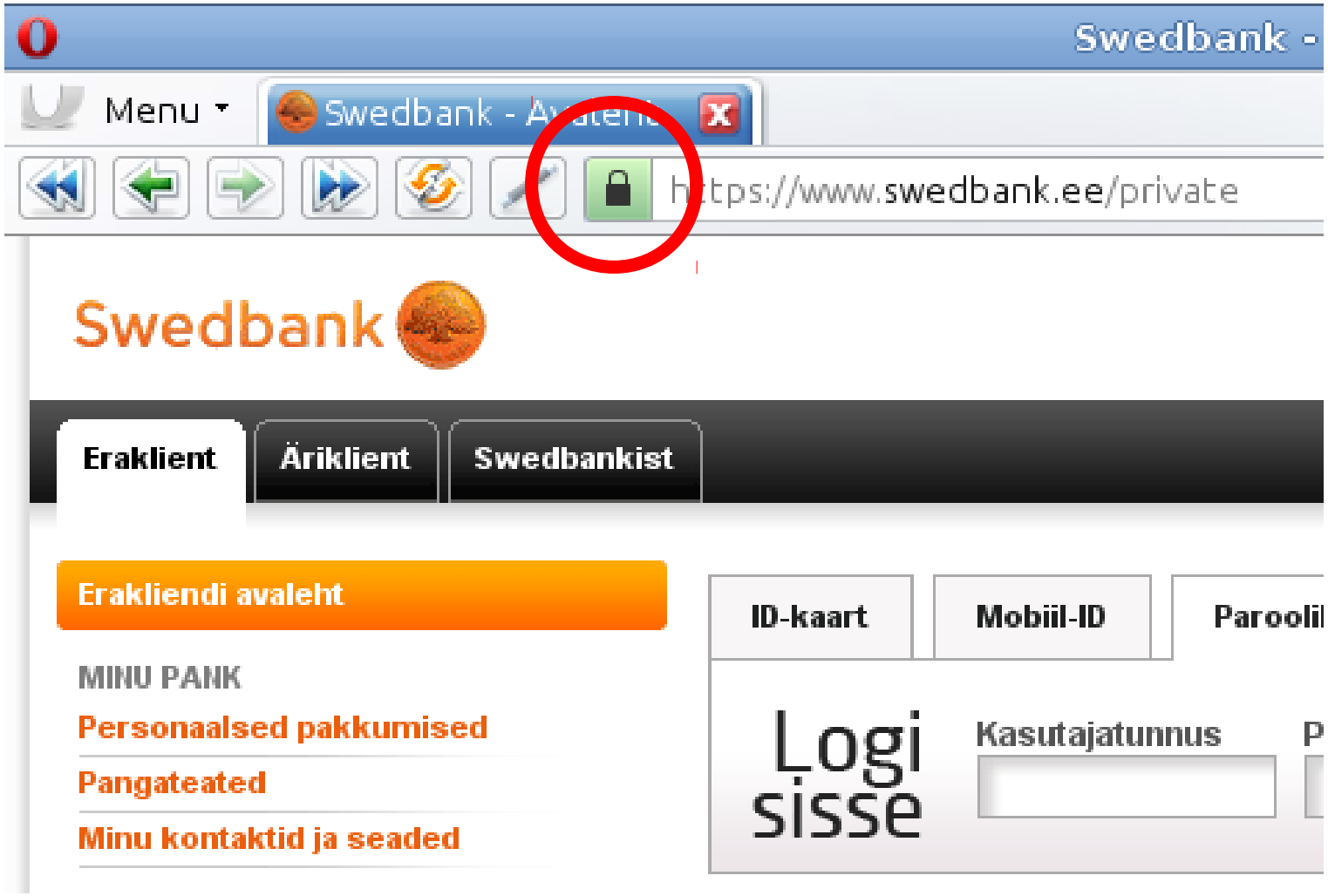
Geeks vs. Humans (2)

- Example of the difference between geeks and normal humans
  - All of Anne's children are blond
  - Does it follow that some of Anne's children are blond?

Geeks vs. Humans (3)

- Most geeks would agree that the inference (a subalternation in Aristotlean logic) from “all A are B” to “some A are B” is valid
- 70% of normal humans consider this invalid
  - This result is consistent across different cultures and rephrasings of the problem (in the jargon, it is robust)
- The people creating the security software just don’t think like the majority of the people using it

Geeks vs. Humans (4)



Security and Rationality

- Our brains evolved for survival and reproduction, not to automatically seek the truth
  - Quick and dirty techniques serve evolution better than purely rational ones
- We can rationalise away almost anything

Security and Rationality (2)

- People will concoct plausible explanations for something and continue to believe it even if they're shown that the evidence for their conclusion is wrong
  - This plays straight into the hands of con artists and phishers

Security and Rationality (3)

- Example: Humans going to a phishing site (part of a phishing study)
  - www.ssl-yahoo.com must be a "subdirectory" of Yahoo!
  - sign.travelocity.com.zaga-zaga.us is probably an outsourcing site for travelocity.com
  - The company running the site probably had to register a different name from its brand because the name was already in use by someone else
  - Other sites use IP addresses instead of domain names so this IP-address-only site must be OK
  - Sites use redirection to a different site so this one must be OK

Security and Rationality (4)

- Extreme example: Patients whose brain hemispheres have been separated in order to treat severe epileptic attacks
  - Split-brain/corpus callosotomy
  - Left brain was able to rationalise away what the right brain was doing even though it literally had no idea why it was doing it
- An example of a phenomenon called illusory correlation
  - People see connections where there aren't any

Security and Rationality (5)

- Self-deception isn't a bug but a psychological defence mechanism
- Depressed people have a better grasp of reality than nondepressed people, not the other way around
  - Phenomenon is called depressive realism
- Depressives suffer from a deficit in self-deception

Security and Rationality (6)

- High levels of self-deception are strongly correlated with conventional notions of good mental health
  - If the self-deception is removed, various mental disorders may emerge
- Some level of irrationality is a fundamental aspect of human nature

The “Simon Says” Problem

- Users are required to change their behaviour in the absence of a stimulus
- Problem is well-known to social psychologists
  - Experts can do this in some cases because they’ll notice the absence of a particular cue
  - Novices don’t know what’s supposed to happen and so won’t notice when it doesn’t happen

The “Simon Says” Problem (2)

- Example: Subjects are shown sets of trigrams with a special feature
  - After (on average) 34 sets of trigrams, they figured out that the special feature was the presence of the letter ‘T’
  - No-one was able to detect the absence of the letter ‘T’, no matter how many trigrams they saw
- This is exactly what browser UI designers expect us to be able to do!
  - We have to detect the absence of a stimulus like a padlock

The "Simon Says" Problem (3)

- People find negative information far more difficult to process than positive information
  - Educational psychologists advise educators to present information as positively-worded truths, not negatively-worded non-facts

The "Simon Says" Problem (4)

- Example: Propositional calculus problems used by psychologists
  - If today is not Wednesday, then it is not a public holiday.
  - Today is not a public holiday.
- Is today not Wednesday?
  - People find these problems far harder to evaluate than positive-information ones
- Example: Browser security indicators
  - If the padlock is not showing then the security is not present.

Inattentional Blindness

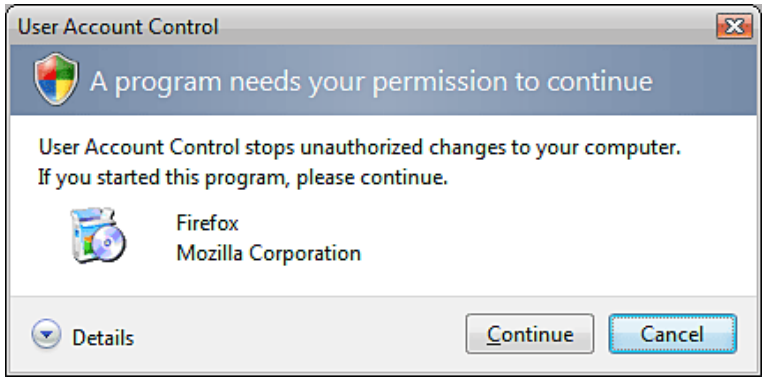
- People don't register objects unless they're consciously paying attention to them
- Best-known example is "Gorillas in our Midst"
  - Subjects were asked to watch a basketball game with players dressed in black and white
  - Told to count the number of times that each team bounced the ball
  - In the middle of the game, a person in a gorilla suite pranced across the court
  - Only 54% of users noticed

Inattentional Blindness and Security

- The padlock and other security indicators are a perfect match for inattentional blindness
  - Researchers have found up to 100% failure rates for these indicators
- IE6 SP2 added a security bar to warn users of security issues
  - One usability test found that not one user had noticed its presence

Inattentional Blindness and Security (2)

- Windows Vista added UAC dialogs to warn users of (potential) security issues



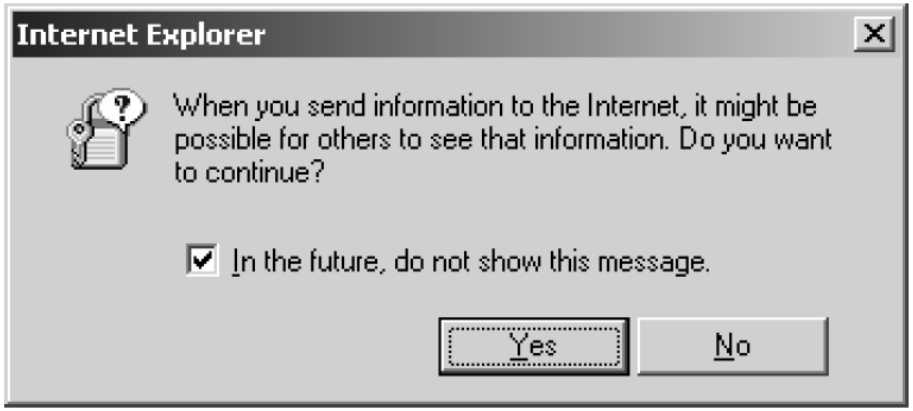
  - Informal tests revealed that no-one had noticed that it had different colours in different situations
  - Now try and find out what the colours actually signify…

User Education

- Security is a nebulous concept that's difficult for users to relate to
  - Removing red-eye in a photo program is a tangible goal with tangible actions
  - "Being secure" is, uhhh, …
- In normal computer usage, users can rely on satisficing
  - Click on something that looks appropriate
  - If it doesn't work, go back and try again

User Education (2)

- This interacts really badly with the way that most applications handle security



  - HCI researchers call these warn-and-continue (WC) dialogs acknowledging that users will click straight past them
  - Dropping problems into a WC is easy for developers but doesn't help keep the user safe

User Education (3)

- User studies have found that users expect the application to make security decisions for them
  - Application developers expect users to make the security decisions
- No-one takes responsibility, because it's the other side's problem

User Education (4)

- Mozilla developer reported WC dialogs as “a chronicle of indecision within the walls of Netscape”
  - Every confirmation window and question to the user marks a case where two internal camps couldn’t agree on the most secure way to proceed and instead deferred to the user
- Firefox developers discovered via feedback from users that they saw through this deception
  - [Warning dialogs are] intentionally obfuscated warnings that companies can point to later and say ‘Look, we warned you!’

User Education (5)

- Conventional human-based error mitigation techniques
  - Pre-selection screening (academic grades, psychological profiles)
  - Selection screening (entrance exams, interviews)
  - Work training
  - On-the-job evaluation
- Computer human-based error mitigation techniques
  - (None)
- No standard mitigation techniques can be applied for any but a very restricted set of uses (the military, SCADA use, etc)

User Education (6)

- Even experimental attempts to train users have run into problems
- In one study, researchers found that training had no effect on users' ability to detect phishing email
  - All it did was scare them into rejecting more email of all types (legitimate and phishing)

User Education (7)

- If user education was going to work, it would have worked by now
  - — Anti-virus researcher Vesselin Bontchev

The Bystander Effect

- Phishers use the bystander effect to build confidence in the phishing sites
  - Provide a hotline number for users to call to check the site authenticity
  - No-one ever calls it, but they trust the site more because of it

- „The 10 Inescapable Truths of Security UI”
  - by Peter Gutmann

The 10 Truths

- Truth #1 (Security UI Prime Directive): If the user can't understand your security interface, it doesn't exist
  - — Clare-Marie Karat, Carolyn Brodie, and John Karat
- Truth #2: Any security message/dialog that can be rephrased as "Do you want to continue to perform your job/intended task?" simplifies to a boolean value of TRUE

The 10 Truths

- Truth #3: Nil utilitatis sine probatione: Any security UI that isn't tested in the real world reduces to Truth #1
  - Truth #3 Corollary: Any security UI that isn't tested for failure conditions as well as success conditions reduces to Truth #1

The 10 Truths

- Truth #4: If your security UI is more complex than username + password → “accepted”/“declined”, you've lost 80% of your user base and your UI reduces to Truth #1
  - Truth #4 Corollary: If your UI involves concepts like certificates, key fingerprints, CAs, and webs of trust, this increases to ~100%

The 10 Truths

- Truth #5: If user education was going to work, it would have worked by now.
  - — Vesselin Bontchev
- Truth #6: A security handshake can have only two possible outcomes, “connected with both sides mutually authenticated” or “not connected”. Anything else is just building substrate for phishing attacks

The 10 Truths

- Truth #7: If a validation check fails then the data or session should be treated as if no security was present, not worse than if no security was present
  - — Phil Hallam-Baker

The 10 Truths

- Truth #8: Security features that are off by default will stay off
  - Truth #8 Corollary 1: Security features that turn themselves off (for example anti-virus subscriptions) will stay off.
  - Truth #8 Corollary 2: Security features that annoy the user and can be turned off will be turned off and stay off

The 10 Truths

- Truth #9: Security UI design is the hardest of all types of UI design. While the typical user can muddle their way through a field sown with cowpats, they can't muddle their way through a field sown with antipersonnel mines
- Truth #10: The best is the enemy of the good: Any effective but less than theoretically perfect security technology will be panned by experts, self-appointed or otherwise

Conclusion

- Humans' minds work very differently from geeks' minds
  - Many applications are written by geeks for geeks
  - (Even supposedly user-friendly ones)
- The mind works in very counterintuitive ways
  - There are good reasons for the behaviour, but they're not at all obvious
- Geeks are weird
  - (No, really)